



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/626,637	07/27/2000	Deepak Gupta	JP920000150US1	9799

39903 7590 08/11/2004

ANTHONY V.S. ENGLAND
1717 WEST SIXTH STREET
SUITE 230
AUSTIN, TX 78703

EXAMINER

SHIN, KYUNG H

ART UNIT	PAPER NUMBER
----------	--------------

2143

DATE MAILED: 08/11/2004

11

Please find below and/or attached an Office communication concerning this application or proceeding.

SL

Office Action Summary

Application No.

09/626,637

Applicant(s)

GUPTA ET AL.

Examiner

Kyung H Shin

Art Unit

2143

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 May 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-6 and 11-19 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-6, 11-19 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. This action is responding to application papers dated 5/27/2004.
2. **Claims 1-6, 11-19** are pending. **Claims 1-5 are amended, claim 7-10 are cancelled, and claims 11-19 are new. Claims 1, 6, and 13 are independent claims.**

Response to Arguments

3. Applicant's arguments filed **7/27/2000** have been fully considered but they are not persuasive in overcoming the rejections based on the prior art of **Lewis et al.** and **Perlman et al.** The applicant have argued the following:

3.1 Lewis discloses "verifying by the browser the original authentication certificate by using the expired public key of the certifying authority" (see Lewis col. 30, lines 39-41: "*When a certificate expires, the USPS certification authority will issue a new certificate and sign it with the old certificates matching private key.*"; col. 27, lines 1-3: "Signing an item with a private key means having the ability to verify it only by using the corresponding public key.") The reference states that when a new public/private key pair is generated for a Certificate Authority (CA) replacing an expired public/private key pair. When an expired private key is used to sign a certificate, the corresponding expired public key must be used to verify the certificate. The reference's authentication process is

equivalent to the applicant's process in the verification of a CA certificate using the expired public key of the CA. This verification and authentication step can be completed by any network entity including one operating a network browser.

3.2 Lewis discloses that "presenting the original valid authentication certificate together with the said server certifying authority chain certificate, by the server to the browser during the SSL handshake." SSL (Secure Socket Layer) is a secure communications protocol between a browser (i.e. server) and a client. (see Lewis col. 14, lines 36-42: " ... *the transaction server ... will employ SSL3.0 (Secure Socket Layer) standard encryption for secure packaging SSL3.0 is an accepted industry standard for financial transactions across a TCP/IP network.*") The reference's secure client-server communications between network entities utilizes the SSL protocol. The invention's secure communications uses the equivalent SSL protocol.

A client browser receives a server certificate and Certificate Authority (CA) certificate plus the digital signatures required for usage in the verification of both certificates. (see Lewis col. 27, lines 10-24: " ... *user A wanted to verify the digital signature of an item issued by B, User A can then verify the authenticity of the X.509 certificate by looking at the digital signature contained as part of the certificate (field 11). ... issued by a trusted third party (Certificate Authority) User A would first*

extract the USPS public key from the X.509 and use that to verify the signature in B's X.509 certificate. If the signature verifies then the X.509 certificate is authentic... , user A can then extract B's public key from the X.509 certificate and similarly verify the digital signature of the item issued by B.") The reference's user A is designated as the client, user B is designated as the server and the USPS is designated as the CA. The server certificate and the Certificate Authority (CA) certificate are both verified by the client's browser. The reference presents for processing the server and CA certificates for verification. The applicant's process performs the presentation of the same server and CA certificates. Therefore, the rejection of claims is proper and maintained herein.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. **Claims 1, 4-6, 11, 13,17-19** are rejected under 35 U.S.C. 102(e) as anticipated by **Lewis et al.** (U.S. Patent No. 6,233,565, Filed Feb. 13, 1998)

Regarding Claim 1 (Currently Amended), Lewis discloses a method for enabling the use by a browser of valid authentication certificates in relation to a

transaction between the browser and a server when a private key and public key of a certifying authority of the server has expired, comprising:

receiving an original authentication certificate together with a server certifying authority chain (SCAC) certificate by the browser from the server during a SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by the server from the certifying authority (see col. 30, lines 39-41)

verifying by the browser the original authentication certificate using the expired public key of the certifying authority, (see col. 14, lines 36-42; col. 30, lines 41-43) and

verifying by the browser the SCAC certificate using a new public key of the certifying authority. (see col. 30, lines 43-50)

Regarding Claim 4 (Currently Amended), Lewis discloses the method of claim 1 further comprising issuing by the certifying authority a client (CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged. (see col. 31, lines 30-38)

Regarding Claim 5 (Currently Amended), Lewis discloses the method of claim 1, wherein the method further comprises presenting the CCAC certificate to the server during the handshake. (see col. 14, lines 36-42; col. 31, lines 14-21)

Art Unit: 2143

Regarding Claim 6 (Original), Lewis discloses in an arrangement of networked server and browser systems conducting secure transactions and including a certifying authority for authenticating such transactions, characterized in that it includes a means for authenticating transactions when the public and private key of the said certifying authority have expired but the authentication certificates of any of server or browser systems is still valid, comprising;

a means for the server to obtain a certifying authority chain certificate using the new private key of the certifying authority, (see col. 30, lines 39-41)

a means for presenting the said certifying authority chain certificate together with the original authentication certificate, to the browser,, (see col. 14, lines 36-42; col. 30, lines 41-43)

a means for verifying the original authentication certificate using the expired public key of the certifying authority, and verifying the certifying authority chain certificate using the new certifying authority public key by the browser. (see col. 30, lines 43-50)

Claims 7-10 (Canceled)

Regarding Claim 11 (New), Lewis discloses the method of claim 1, further comprising accepting the transaction by the browser after said verifying the original authentication certificate and after said verifying the SCAC certificate. (see col. 27, lines 10-24)

Regarding Claim 12 (New), Lewis discloses the method of claim 1, wherein obtaining the SCAC certificate comprises using the new private key of the certifying authority. (see col. 30, lines 41-43)

Regarding Claim 13 (New), Lewis discloses a system for enabling use by a browser of valid authentication certificates in relation to a transaction between the browser and a server when a private key and public key of a certifying authority of the server has expired, comprising:

means for receiving an original authentication certificate together with a server certifying authority chain (SCAC) certificate by the browser from the server during a SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by the server from the certifying authority; (see col. 27, lines 10-24)

means for verifying by the browser the original authentication certificate using the expired public key of the certifying authority; (see col. 30, lines 39-41) and

means for verifying by the browser the SCAC certificate using a new public key of the certifying authority. (see col. 30, lines 41-43)

Regarding Claim 17 (New), The system of claim 13, wherein the system further comprises means for presenting the CCAC certificate to the server during the handshake. (see col. 27, lines 10-24)

Regarding Claim 18 (New), The system of claim 13, further comprising means for accepting the transaction by the browser in conjunction with said means for verifying the original authentication certificate and in conjunction with said means for verifying the SCAC certificate. (see col. 27, lines 10-24)

Regarding Claim 19 (New), The system of claim 13, wherein said means for obtaining the SCAC certificate comprises use of the new private key of the certifying authority. (see col. 30, lines 41-43)

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. **Claims 2, 3, 14-16** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Lewis et al.** (U.S. Patent No. 6,233,565: File date is Feb. 13, 1998) in view of **Perlman et al.** (U.S. Patent No. 6,230,266: File date is Feb. 3, 1999).

Regarding Claim 2 (Currently Amended),

Lewis discloses a Certificate Authority (CA) for the distribution of certificates used in the verification of client and server systems. Lewis does not disclose a

Art Unit: 2143

Certificate Authority (CA) that invalidates or withdraws its public/private key.

However, **Perlman** discloses a Certificate Authority (CA) that invalidates or withdraws its public/private key pair through the process of revocation. Further, Perlman discloses the method of claim 1, wherein the SCAC certificate is obtained by the server whenever the certifying authority invalidates its public key, wherein the certificate is obtained by:

contacting the certifying authority using the server's private key for authentication to make a request for the SCAC certificate; (see col. 6, line 63 - col. 7, line 6)

verifying the request by the certifying authority using the server's public key; and (see col. 7, lines 15-18)

generating the SCAC certificate by the certifying authority using its new private key of the certifying authority and forwarding the SCAC certificate to the server. (see col. 7, lines 12-24)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inventions of *Lewis* to include a Certificate Authority (CA) that invalidates its key pair through the process of revocation as taught in *Perlman*. One of ordinary skill in the art would have been motivated to incorporate the invention of *Perlman* in order to ensure the authenticity of certificates when a CA invalidates a public/private key pair due to a compromise in security. (see *Perlman* col. 2, lines 20-26: *"For complete network security, every principal must have a certificate. Sometimes, however, it is desirable to later disable a certificate after it has been issued but prior to its expiration. For*

Art Unit: 2143

example, a principal's private key may be stolen, compromised or lost, etc. Under such circumstances, it is desirable to revoke the certificate, thereby disabling authentication via that certificate.")

Regarding Claim 3 (Currently Amended),

Lewis discloses a Certificate Authority (CA) for the distribution of certificates used in the verification of client and server systems. Lewis does not disclose usage of the server name and public key, CA name and public key in the authentication process. However, Perlman discloses the method of claim 2 wherein generating the SCAC certificate includes authenticating the server name, the server public key, old certifying authority public key and certifying authority name. (see Perlman col. 7, lines 10-12)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inventions of *Lewis* to include the invention of *Perlman*. One of ordinary skill in the art would have been motivated to employ the invention of *Perlman* to *Lewis* in order to use efficiently the server name and public key, CA name and public key in authentication. (see *Perlman* col. 1, line 65 - col. 2, line 9: "*It is essential to reliably know which public key belongs to which principal. ... CA generates identity certificates, ... specifying ... , the name of the principal whose public key is being certified, the certificate serial number, name of the CA issuing the certificate, the subject's public key, and also, typically, a certificate expiration date. This verification of the relationship between the public key and the principal to which it belongs precludes an intruder from*

compromising the system by posing as a valid principal.”; col. 7, lines 10-12: “
... , the new CA 204b is configured to issue certificates in the same name as the
CA 204a.”) The compromise of a CA and its identifying information requires
another CA and its identifying information to assume the certificate verification
process.

Regarding Claim 14 (New), Lewis does not disclose a Certificate Authority (CA)
invalidation of its public/private key. However, Perlman discloses the system of
claim 13, wherein the SCAC certificate is obtained by the server whenever the
certifying authority invalidates its public key, wherein the certificate is obtained
by:

means for contacting the certifying authority using the server's private key
for authentication to make a request for the SCAC certificate; (see
Perlman col. 6, line 63 - col. 7, line 6)

means for verifying the request by the certifying authority using the
server's public key; (see Perlman col. 7, lines 15-18) and

means for generating the SCAC certificate by the certifying authority using
a new private key of the certifying authority and forwarding the SCAC
certificate to the server. (see Perlman col. 7, lines 12-24)

It would have been obvious to one of ordinary skill in the art at the
time of the invention to modify the inventions of *Lewis* to include a
Certificate Authority (CA) that invalidates its key pair as taught in *Perlman*.
One of ordinary skill in the art would have been motivated to incorporate

the invention of Perlman in order to ensure the authenticity of certificates when a CA invalidates a public/private key pair due to a compromise in security. (see Perlman col. 2, lines 20-26)

Regarding Claim 15 (New), Lewis discloses a Certificate Authority (CA) for the distribution of certificates used in the verification of client and server systems. Lewis does not disclose usage of the server name and public key, CA name and public key in the authentication process. However, Perlman discloses the system of claim 13, wherein said means for generating the SCAC certificate includes means for authenticating the server name, the server public key, old certifying authority public key, and certifying authority name. (see Perlman col. 7, lines 10-12)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inventions of *Lewis* to employ the certificate includes the authentication of the server name, the server public key, old CA public key and CA name as taught in *Perlman*. One of ordinary skill in the art would have been motivated to incorporate the invention of Perlman to Lewis in order to efficiently and securely re-establish authentication system by using the server name and public key, CA name and public key in authentication. (see Perlman col. 3, lines 54-63)

Regarding Claim 16 (New), Lewis discloses the system of claim 15, further comprising means for issuing by the certifying authority a client (CCAC) certificate, said CCAC certificate being functionally the same as the SCAC

Art Unit: 2143

certificate subject to the roles of the browser and the server being interchanged.

(see Lewis col. 30, lines 59-62)

Conclusion

8. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H Shin whose telephone number is 703-305-0711. The examiner can normally be reached on 9 am - 7 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A Wiley can be reached on 703-308-5221. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

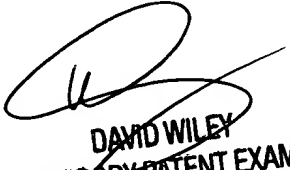
Art Unit: 2143

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KHS

Kyung H Shin
Patent Examiner
Art Unit 2143

KHS
Aug. 5, 2004



DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100